This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/709,839	11/10/2000	Dylan Smith	CHA9-2000-0002US1	4445

23550 7590 09/14/2004

HOFFMAN WARNICK & D'ALESSANDRO, LLC
3 E-COMM SQUARE
ALBANY, NY 12207

EXAMINER	
ZAND, KAMBIZ	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/709,839	SMITH, DYLAN	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 November 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *04/12/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-28** have been examined.

Drawings

2. Examiner accepts drawings filed on 11/10/2000.

Information Disclosure Statement PTO-1449

3. The Information Disclosure Statement submitted by applicant and received on 04/12/2001 has been considered. Please see attached PTO-1449. Note: The records of IFW files disclose the submission of IDS on 11/10/2000 and **exact duplicate** submitted again on 11/30/2000 with received date of 04/12/2001.

Claim Objections

4. **Claims 18 and 27** are objected to because of the following informalities: typo error. Examiner suggests the following corrections:

Claim 18:

- Please replace the phrase "claim 18" line 1 with the phrase "claim 17".

Claim 27:

- Please insert the phrase "to" after the phrase "external" line 1.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. **Claims 1-5, 9-12, 14-15, 17, 18, 20-28** are rejected under 35 U.S.C. 102(b) as being anticipated by Hodges et al (6,035,423 A).

As per claim 1 Hodges et al (6,035,423 A) teach a method of conducting non-authentication tasks using an authentication system of a workstation, comprising the steps of: loading a task module to the authentication system of the workstation **(see col.7, lines 15-17 and 33-40 disclose downloading a task module for upgrading antivirus application to client or workstation system where it is an authenticated system since it logon by using client's id and ip address)**; and conducting a non-authentication task using the task module **(see col.5, lines 23-33 where it disclose upgrading antivirus application**

automatically; col.7, lines 53-67 disclose a non-authentication task by providing a flash notification to be seen by the user where user may decide on immediate installation or postpone the process to a later time where no user logon is necessary).

As per claim 2 Hodges et al (6,035,423 A) teach the method of claim 1, wherein the step of conducting a non-authentication task includes: logging onto the workstation using the task module as requested by an upgrade **(see col.7, lines 28-40 where logon using update antivirus application agent that corresponds to Applicant's task module is being processed)**; and automatically upgrading an application on the workstation **(see col.5, lines 23-33 where it disclose upgrading antivirus application automatically; col.7, lines 48-53).**

As per claim 3 Hodges et al (6,035,423 A) teach the method of claim 2, further comprising the step of displaying a message indicating an upgrade status **(see col.7, lines 53-62 where there is an option to send a message called flash notification to the user with respect to upgrade status).**

As per claim 4 Hodges et al (6,035,423 A) teach the method of claim 3, further comprising the step of sending a response to the message to the upgrade from a user of the workstation **(see col.7, lines 58-60 where the user has the option**

of response by selecting immediate downloading or later downloading of upgrade files).

As per claim 5 Hodges et al (6,035,423 A) teach the method of claim 2, wherein the step of logging on to the workstation occurs without user interaction **(see col.7, lines 45-53 where the downloading and updating is automatic on client computer; col.7, lines 64-67 and col.8, lines 1-5 where the updating is being processed in the background of the user's workstation or terminal without user interaction, therefore the process of logging to the terminal and auto executing of updated program is without user interaction since the credential of the user is already received by antivirus server that uses push up technology to update the applications as depicted further in col.7, lines 32-43 automatically).**

As per claim 9 Hodges et al (6,035,423 A) teach the method of claim 1, wherein the step of conducting the non-authentication task includes displaying a message from a requester **(see col.7, lines 44-60 where the agent within the anti virus application corresponds to Applicant's requestor sending optionally a message for display to the user notifying the status of the update by giving the client or user or workstation two options to choose).**

As per claim 10 Hodges et al (6,035,423 A) teach the method of claim 9, further comprising the step of sending a response to the message to the requester from

a user of the workstation **(see col.7, lines 58-60 where the user respond to the message display by choosing one of the two options available sent by the agent that also corresponds to Applicant's requestor).**

As per claim 11 Hodges et al (6,035,423 A) teach the method of claim 1, wherein the step of conducting the non-authentication task includes logging onto the workstation using the task module as requested by a requester **(see claim 2 above; also see col.7, line 28-39 where the agent corresponds to the requestor and antivirus application corresponds to the task module).**

As per claim 12 Hodges et al (6,035,423 A) teach the method of claim 1, wherein the loading step includes a requester instructing a task module loader of the authentication system to load the task module **(see col.7, lines 28 where the agent within antivirus application upgrade corresponds to the requester, line 48-58 where the instruction for downloading of the antivirus application update that corresponds to the task module is being processed and where there be inherently a loader in order to download the application).**

As per claim 14 Hodges et al (6,035,423 A) teach the method of claim 12, wherein the task module is delivered via a command pipe **(see the task module delivered through a link (fig.2 communication link 204 and fig.3 communication link to workstation 302).**

As per claim 15 Hodges et al (6,035,423 A) teach the method of claim 1, wherein the step of loading occurs without interrupting workstation operation **(see col.7, lines 66-67 and col.8, lines 1-5 where the step of loading is being done in the background and transparent to the user).**

As per claim 17 Hodges et al (6,035,423 A) teach a computer program product comprising a computer useable medium having computer readable program code embodied therein for conducting non- authentication tasks using an authentication system of a workstation **(see col.6, lines 11-16 disclose the client 302 that corresponds to Applicant's workstation having Pentium processor running on operating system windows 95 that corresponds to one type of software program stored and col.8, lines 6-7 disclose the client computer having a hard disk that corresponds to Applicant's memory where the computer readable media corresponds to the client hard disk or memory for carrying the computer product such as the operating system program 95 or antivirus application)**, the computer program Product Comprising: a task module configured to conduct a non-authentication task **(see col.5, lines 23-33; col.7, lines 15-17, 33-60 disclose configured a task module for upgrading antivirus application to client or workstation system; and where it is non-authentication task includes upgrading antivirus application automatically and by providing a flash notification to be seen by the user where user may decide on immediate installation or postpone**

the process to a later time); and a task module loader configured to load the task module **(see col.7, lines 28 where the agent within antivirus application upgrade corresponds to the requester, line 48-58 where the instruction for downloading of the antivirus application update that corresponds to the task module is being processed and where there be inherently a loader in order to download the application)** to the authentication system of the workstation **(see col.7, lines 33-40 where it is an authenticated system since it logon by using client's id and ip address)**.

As per claim 18 Hodges et al (6,035,423 A) teach the computer program product of claim 18, wherein the task module loader is stored in the authentication system of the workstation **(see claim 17 above with respect to loader; also see col.8, lines 6-35 disclose storing the applications in the client computer where the execution of a an application such as antivirus update program is executed; col.9, lines 1-10 disclose execution of tasks where the file are executable by themselves and as mentioned they are resident within the workstation and where there be inherently a loader in order to download the application loads the update software are located within the program and the program is resident within the client computer or workstation).**

As per claims 20 and 27, Hodges et al (6,035,423 A) teach the computer program product of claims 18 and 25, wherein the task module is loadable from

an external requester which is external to the workstation **(see col.7, lines 28-36 where the task module is loadable originally from the server which corresponds to external requester through the update agent that acts as internal requester within the workstation).**

As per claim 21 Hodges et al (6,035,423 A) teach the computer program product of claim 18, further comprising a request receiver configured to receive a request to load the task module from a requester **(see col.7, lines 28 where the agent within antivirus application upgrade corresponds to the requester, line 48-58 where the instruction for downloading of the antivirus application update that corresponds to the task module is being processed and it is loaded to the receiver at the client computer).**

As per claim 22 Hodges et al (6,035,423 A) teach the computer program product of claim 18, wherein the task module includes a logon system configured to conduct a userless logon of the workstation **(see col.7, lines 45-53 where the downloading and updating is automatic on client computer; col.7, lines 64-67 and col.8, lines 1-5 where the updating is being processed in the background of the user's workstation or terminal without user interaction, therefore the process of logging to the terminal and auto executing of updated program is without user interaction since the credential of the user is already received by antivirus server that uses push up technology to**

update the applications as depicted further in col.7, lines 32-43 automatically).

As per claim 23 Hodges et al (6,035,423 A) teach the computer program product of claim 18, wherein the task module includes a display system configured to display a message on a sign-on screen of the workstation **(see col.7, lines 44-60 where the agent within the anti virus application corresponds to Applicant's requester sending optionally a message for display to the user notifying the status of the update by giving the client or user or workstation two options to choose).**

As per claim 24 Hodges et al (6,035,423 A) teach the computer program product of claim 23, wherein the display system is further configured to send a response to a message from a workstation user to a requester **(see col.7, lines 58-60 where the user respond to the message display by choosing one of the two options available sent by the agent that also corresponds to Applicant's requestor).**

As per claim 25 Hodges et al (6,035,423 A) teach an apparatus **(see fig.3)** for conducting non-authentication tasks **(see col.5, lines 23-33; col.7, lines 48-62 disclose non-authentication task includes upgrading antivirus application automatically and by providing a flash notification to be seen by the user where user may decide on immediate installation or postpone the process**

to a later time where no user logon is necessary), using an authentication system of a workstation **(see col.7, lines 33-40 disclose a client or workstation system where it is an authenticated system since it logon by using client's id and ip address)**, the apparatus comprising: a task module configured to conduct a non-authentication task using the authentication system **(see col.5, lines 23-33; col.7, lines 15-17, 33-60 disclose configured a task module for upgrading antivirus application to client or workstation system where it is an authenticated system since it logon by using client's id and ip address; and where it is non-authentication task includes upgrading antivirus application automatically and by providing a flash notification to be seen by the user where user may decide on immediate installation or postpone the process to a later time where no user logon is necessary)**; a task module loader resident in the authentication system configured to load the task module; and a requester configured to instruct the task module loader to load the task module and to instruct the authentication system how to activate the task module **(see col.7, lines 28 where the agent within antivirus application upgrade corresponds to the requester, line 48-58 where the instruction for downloading of the antivirus application update that corresponds to the task module is being processed and where there be inherently a loader in order to download the application)**.

As per claim 26 Hodges et al (6,035,423 A) teach the apparatus of claim 25, wherein the requester is one of an upgrade system and an upgrade program

(see col.7, lines 44-60 where the agent within the anti virus application corresponds to Applicant's requester that initiate the application upgrade process which corresponds to Applicant's one of an upgrade system; and the application itself such as antivirus application corresponds to Applicant's upgrade program).

As per claim 28 Hodges et al (6,035,423 A) teach a workstation **(see col.6, line 11-13 where the client computer 302 corresponds to Applicant's workstation)**, comprising: A processor, and memory, having a software program stored therein, and executable by the processor **(see col.6, lines 11-16 disclose the client 302 that corresponds to Applicant's workstation having Pentium processor running on operating system windows 95 that corresponds to one type of software program stored and col.8, lines 6-7 disclose the client computer having a hard disk that corresponds to Applicant's memory),** the software program including: an authentication system **(see col.7, lines 33-40 disclose a client or workstation system where it is an authenticated system since it logon by using client's id and ip address)**; a task module configured to conduct a non-authentication task using the authentication system **(see col.5, lines 23-33; col.7, lines 15-17, 33-60 disclose configured a task module for upgrading antivirus application to client or workstation system where it is an authenticated system since it logon by using client's id and ip address; and where it is non-authentication task includes upgrading antivirus application automatically and by providing a flash notification to be seen**

by the user where user may decide on immediate installation or postpone the process to a later time where no user logon is necessary), a task module loader resident in the authentication system configured to load the task module; and a requester configured to instruct the task module loader to load the task module and to instruct the authentication system how to activate the task module **(see col.7, lines 28 where the agent within antivirus application upgrade corresponds to the requester, line 48-58 where the instruction for downloading of the antivirus application update that corresponds to the task module is being processed and where there be inherently a loader in order to download the application)**.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 6, 8, 13, 16 and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over Hodges et al (6,035,423 A) in view of Mohammed (6,418,555 B2) .

As per claim 6 Hodges et al (6,035,423 A) teach all limitation of the claim as applied to the method of claim 2 but do not disclose explicitly the step of automatically rebooting the workstation when the upgrade is complete. However Mohammed (6,418,555 B2) disclose the step of automatically rebooting the workstation when the upgrade is complete **(see fig.2; col.3, lines 13-18 where the rebooting process after upgrade of a program is detailed and line 27-30 where it disclose the rebooting could be automatic)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Mohammed's auto-rebooting method after completion of a program upgrade in Hodges's automatic software updating in order that the device drivers or other software modules for the newly installed software can be reloaded.

As per claim 8 Hodges et al (6,035,423 A) teach all limitation of the claim as applied to the method of claim 1 but do not disclose explicitly the step of automatically rebooting the workstation when the non-authentication task is complete. However Mohammed (6,418,555 B2) disclose the step of automatically rebooting the workstation when the automatic upgrade is complete **(see fig.2; col.3, lines 13-18 where the rebooting process after upgrade of a program is detailed and line 27-30 where it disclose the rebooting could be automatic)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Mohammed's auto-rebooting method after completion of a program upgrade in Hodges's automatic software updating in

order that the device drivers or other software modules for the newly installed software can be reloaded.

As per claim 13 Hodges et al (6,035,423 A) teach all limitation of the claim as applied to the method of claim 12 above but do not disclose explicitly that the task module is in a workstation registry. However Mohammed (6,418,555 B2) disclose that the task module is in a workstation registry **(see fig.3A-B where in order to upgrade the program checks the registry to see if upgrade is needed and in 3b if needed the process is initiated by retrieving registry entry command; col.3, lines 18-67 and col.4, lines 1-35 is detailed that the registry contains the upgrade command that is the task module and the upgrade is being initiated by comparison of the values within the registry to determine if upgrade needed or not)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Mohammed's upgrade task within its registry in Hodges's automatic software updating in order to compare the registry values such as the values of new platform and original platform in order to determine if an upgrade is needed if the two values do not match.

As per claim 16 Hodges et al (6,035,423 A) teach all the limitation of the method of claim I as applied above but do not disclose explicitly the authentication system comprises a graphical identification and authentication dynamic link library. However Mohammed (6,418,555 B2) disclose authentication system

comprises a graphical identification and authentication dynamic link library **(see col.2, lines 40-51 where it disclose having dynamic link library; fig.7 disclose image processing program and identification of associated device where the devices related to image processing corresponds to Applicant's graphical identification).** It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Mohammed's graphical ids and dynamic link library in Hodges's automatic software updating system and method in order to have an upgrade module of self-extracting executable that has various components of the software and different version of the device drivers.

As per claim 19 Hodges et al (6,035,423 A) teach all limitation of the claim as applied to the computer program product of claim 18 above but do not disclose explicitly the task module is loadable from a registry of the workstation. However Mohammed (6,418,555 B2) disclose the task module is loadable from a registry of the workstation **(see fig.3A-B where in order to upgrade the program checks the registry to see if upgrade is needed and in 3b if needed the process is initiated by retrieving from the registry the registry entry command for upgrading; col.3, lines 18-67 and col.4, lines 1-35 is detailed that the registry contains the upgrade command that is the task module and the upgrade is being initiated by comparison of the values within the registry to determine if upgrade needed or not).** It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize

Mohammed's upgrade task within its registry in Hodges's automatic software updating in order to compare the registry values such as the values of new platform and original platform in order to determine if an upgrade is needed if the two values do not match.

9. **Claims 7** is rejected under 35 U.S.C. 103(a) as being unpatentable over Hodges et al (6,035,423 A) in view of Kullick et al (5,764,922 A) cited in the IDS by Applicant.

As per claim 7 Hodges et al (6,035,423 A) teach all limitation of the method of claim 1 as applied above but do not explicitly disclose step of removing the task module when the non-authentication task is complete. However Kullick et al (5,764,922 A) disclose method and apparatus for automatic software replacement where upon the completion of the non-authentication task then task module is removed **(see col.5, lines 2-24 where after renaming the new version installed the old version is removed or relocated to different part of the memory and lunch process continue as normal that is the removal of the task module such as updating of a program)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Kullick's removal or relocation of the old version program from memory and subsequent normal lunching due to removal of the task of the upgrade into Hodges's antivirus auto upgrade method in order to be able to reside the new

upgraded antivirus version as replacement of the old version in an individual computer such as workstation for continuation of normal processing.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

a. U.S.Patent No. US (6,421,781 B1) teach method and apparatus for maintaining security in push server.

b. U.S.Patent No. US (6,178,511 B1) teach coordinating user target logons in a single sign-on environment.

c. U.S.Patent No. US (6,009,274 A) teach method and apparatus for automatically updating software components on end system over a network.

d. U.S.Patent No. US (6,421,768 B1) teach method and system for authentication and single sign on using cryptographically assured cookies in a distributed computer environment.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by

telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

09/07/04

AU 2132